

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
26 February 2004 (26.02.2004)

PCT

(10) International Publication Number
WO 2004/017183 A2

(51) International Patent Classification⁷: **G06F 1/00**

[GB/GB]; Star Internet, Brighthouse Court, Barmwood,
Gloucester GL4 3RT (GB).

(21) International Application Number:

PCT/GB2003/003476

(74) Agents: **AYERS, Martyn, Lewis, Stanley et al.**; J.A.
Kemp and Co., 14 South Square, Gray's Inn, London
WC1R 5JJ (GB).

(22) International Filing Date: 11 August 2003 (11.08.2003)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

0218993.4

14 August 2002 (14.08.2002) GB

(71) Applicant (for all designated States except US): **MES-
SAGELABS LIMITED** [GB/GB]; 1270 Landsdowne
Court, Gloucester Business Park, Gloucester GL3 4AB
(GB).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC,
SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

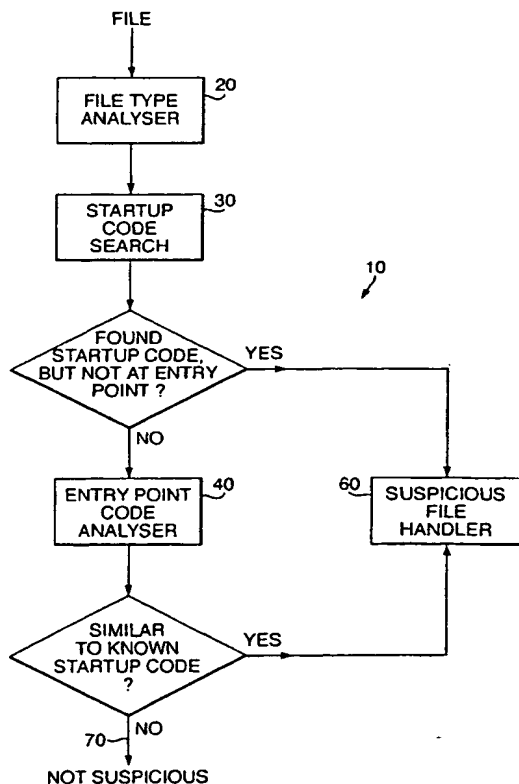
(84) Designated States (*regional*): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,

(72) Inventor; and

(75) Inventor/Applicant (for US only): **SHIPP, Alexander**

[Continued on next page]

(54) Title: **METHOD OF AND SYSTEM FOR, HEURISTICALLY DETECTING VIRUSES IN EXECUTABLE CODE**



(57) Abstract: A method of, and system for, virus detection has a database of known patterns of start-up code for executable images created using a collection of known compilers and uses examination of the start-up code of the image by reference to this database to determine whether or not the executable image is likely to have been subject to infection by viral code. In particular, the system seeks to determine whether the expected flow and execution of the image during start up has had viral code interjected into it. Various heuristics to assist in assessing the likely presence of viral code are disclosed.

WO 2004/017183 A2